UNKNOWN 360 EMAIL TEST REPORT

TESTING MALWARE CATCH RATE OF LEADING EMAIL SECURITY SOLUTIONS

INTRODUCTION

Organizations today are experiencing previously unseen volumes of email traffic. This is in part due to the shift to remote working because of the recent Covid-19 pandemic. As such, email has become an increasingly lucrative target for cyber attackers. Phishing, impersonation, and malware attacks are all rampant, and most organizations are still only marginally protected against these types of attacks. According to a recent Cyber Security Statistics report from PurpleSec (https://tinyurl.com/4dmf3zv7), 92% of malware is delivered by email. Much of this malware is ransomware, and in fact, in 2020 alone, there were over 304m global ransomware attacks and 127 newly discovered ransomware families. (https://www.statista.com/topics/4136/ransomware/)

In this report, we'll discuss the research and findings, the importance of scanning for malware and ransomware, and why basic AV scanning isn't enough. As this report shows, securing your enterprise without proper malware protection is a recipe for disaster. Some of today's most popular email security solutions do not effectively scan for unknown malware, and don't have the experience necessary to block sophisticated malicious attachments. Without proper malware scanning, organizations leave themselves vulnerable to ransomware and other harmful attacks.

Across 4 vendors, including Check Point, Microsoft, Mimecast, and Proofpoint, Check Point security solutions led with the industry's best catch rate of 98.3%, followed by Microsoft at 90%.

ACROSS 4 LEADING EMAIL SECURITY VENDORS, CHECK POINT SECURITY SOLUTIONS LED WITH INDUSTRY'S BEST CATCH RATE FOR UNKNOWN MALWARE

TEST OVERVIEW

Check Point research analysts downloaded a sample set of 360 well-known malicious PDF, DOC, XLS and executable files from Google's "VirusTotal" database. They then used a simple technique to create new and unknown variants (hence the "Unknown 360") from existing malware. The resulting 360 samples preserved the original malicious functionality but are unknown and unregistered in any hash-based database such as VirusTotal. With this set of unknown malware samples, the analysts tested Check Point and other vendors' solutions ability to detect new and unknown malware.

TESTED VENDORS

- Check Point Harmony Email & Office – Anti-phishing, Anti-Malware, Sandbox, CDR
- Microsoft Defender ATP O365 Plan 2 – Anti-phishing, Anti-Malware, Sandbox, CDR
- Mimecast M2 Integrated Email Security – Anti-phishing, Anti-Malware, Sandbox, CDR
- Proofpoint Business Essentials – Anti-phishing, Anti-Malware

To ensure the test validity, platforms were updated with the latest updates available from each vendor as of mid-June 2021. The test configuration also matched the vendor's best practices. The only objective of the test was to test the catch rate of malicious files. Performance was not tested and did not influence the test results in any way.

MICROSOFT AND MIMECAST SANDBOX CANNOT DETECT EVASIVE MALWARE

MIMECAST IS INEFFECTIVE AT DETECTING MALICIOUS PDF DOCUMENTS

MICROSOFT MISSED 3 OUT OF EVERY 10 MALICIOUS EXECUTABLE FILES

MICROSOFT CDR STILL ALLOWS USERS TO CLICK MALICIOUS LINKS

PROOFPOINT IS VERY WEAK IN DETECTING EXES AND HAS NO CDR CAPABILITY

SECURITY FINDINGS

As the Check Point research analysts were conducting the "Unknown 360" test, they came across several security findings that are important to the subject of email-borne malware, and ransomware in email is a huge concern – in 2019, ransomware in phishing emails increased 109%. (https://tinyurl.com/adw2zew)

File Sandboxing

Each vendor provides a cloud-based sandbox solution that serves to evaluate and analyze previously undiscovered files for malicious content and/or activity. As the results show, Check Point's Harmony solution provides a much superior catch rate, with CPU-level detection, AI capabilities, and real-time threat intelligence gathered from millions of global sensors. See more information on the industry-leading Check Point Sandblast Threat Emulation here.

Content Disarm & Reconstruction (CDR)

Content Disarm & Reconstruction is a relatively new feature that provides real-time sanitization of document files as they are being delivered. This allows the end user to avoid waiting for the time-consuming sandboxing process to be completed in order to have a usable file. During testing, it was observed that Microsoft's solution only provided a preview version of the file, while still allowing the user to click on malicious links, negating the value of sandboxing. The Mimecast solution was able to provide a clean version of files; however, because of the inferior catch rate for certain file types, the end user is able to request the original malicious file, rendering the CDR version useless. Proofpoint does not provide this capability, which means users must wait on average 3-5 minutes for full analysis to receive attachments.

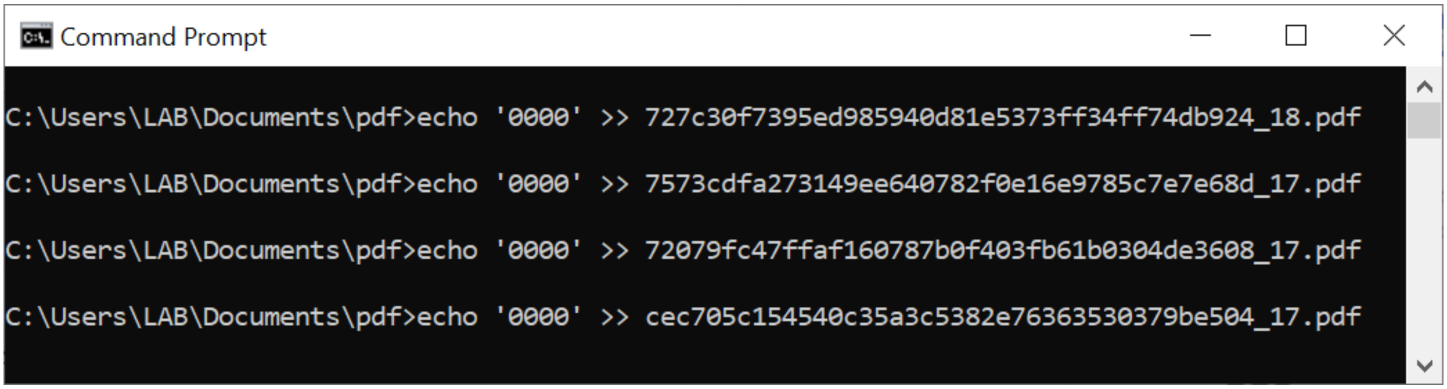
Attachment File Type

As previously discussed in the Test Overview section, this test included 360 files, divided evenly between DOC, PDF, XLS, and EXE types. Not surprisingly, Check Point Harmony Email & Office had the highest catch rate across all file types – 98.3%. Microsoft Defender for O365 fell short in detecting malicious EXE file types, performing at only 70%. Mimecast failed to even deliver a decent catch rate for malicious PDF file types, coming in at only 13.3% effectiveness! Proofpoint did well with documents, but was very inefficient with EXE types, with only a 63.3% catch rate!

CREATING THE UNKNOWN360 TEST METHODOLOGY

To develop the unknown malware test, the researchers queried VirusTotal for pdf, doc, xls and portable executable files that were detected as malicious by at least 10 antivirus engines, in other words, **known** malware. All candidate files were recently uploaded to VirusTotal and demonstrated various malicious behaviors. From this selection, 360 files were randomly chosen (90 PDF, 90 EXE, 90 XLS, and 90 DOC).

After testing solutions using these 360 **known** malware files, Check Point research analysts added a null to the end of each PDF, XLS, and DOC file (e.g. "echo `0000' >> 1.doc"). See *Figure 1* below. In addition, an "unused" header section was modified on each executable file. The analysts then opened and ran each file to validate that the original behavior was kept unchanged. For the executables, a free tool named LordPE was used to change the checksum as shown in *Figure 2* (below). You can find a regularly updated repository of malicious files at https://poc-files.threat-cloud.com to recreate this test in your own lab.



Command Prompt

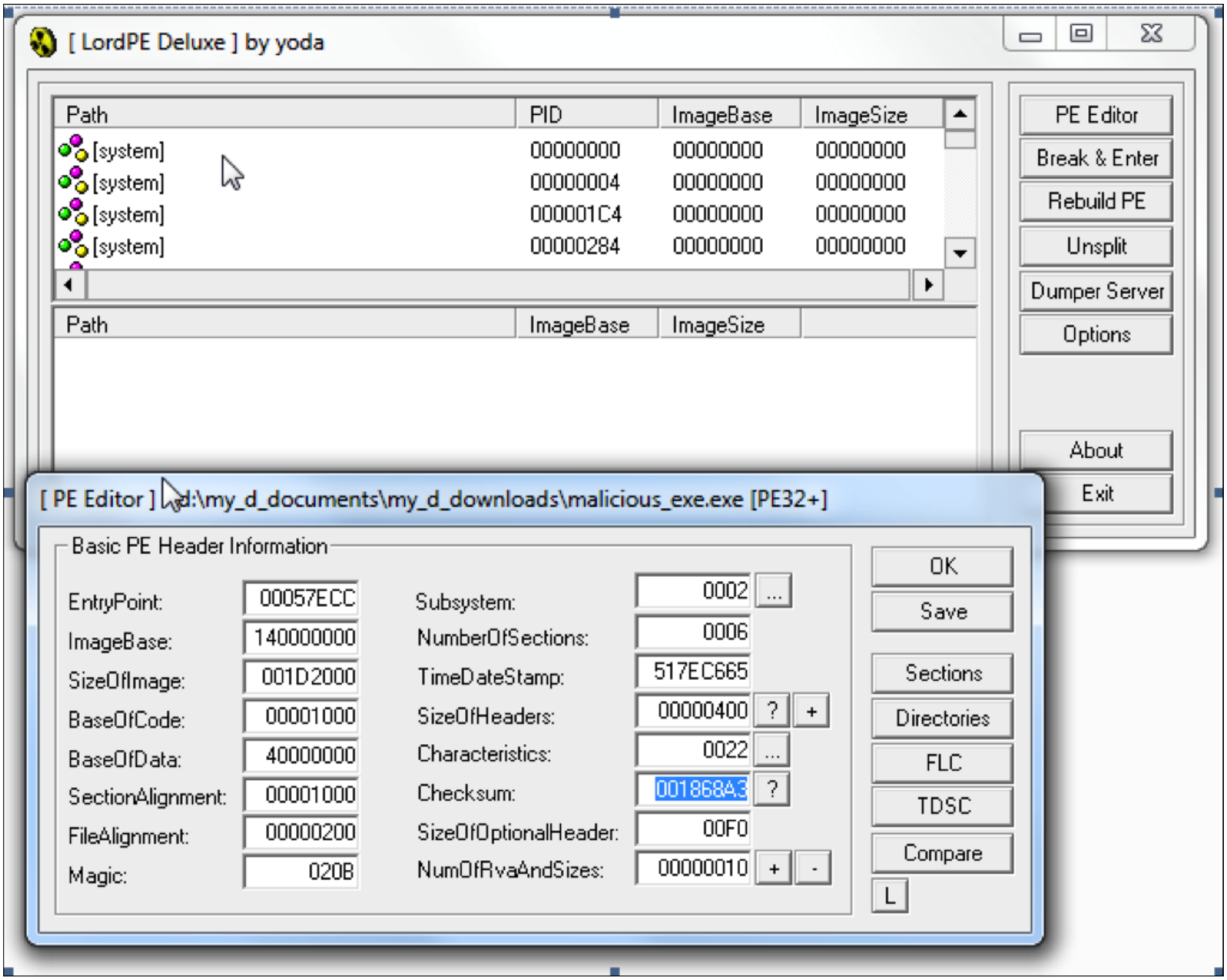
```
C:\Users\LAB\Documents\pdf>echo '0000' >> 727c30f7395ed985940d81e5373ff34ff74db924_18.pdf

C:\Users\LAB\Documents\pdf>echo '0000' >> 7573cdfa273149ee640782f0e16e9785c7e7e68d_17.pdf

C:\Users\LAB\Documents\pdf>echo '0000' >> 72079fc47ffaf160787b0f403fb61b0304de3608_17.pdf

C:\Users\LAB\Documents\pdf>echo '0000' >> cec705c154540c35a3c5382e76363530379be504_17.pdf
```

Figure 1: Manipulating documents using echo command



[LordPE Deluxe] by yoda

Path	PID	ImageBase	ImageSize
[system]	00000000	00000000	00000000
[system]	00000004	00000000	00000000
[system]	000001C4	00000000	00000000
[system]	00000284	00000000	00000000

Path	ImageBase	ImageSize

[PE Editor] d:\my_d_documents\my_d_downloads\malicious_exe.exe [PE32+]

Basic PE Header Information

EntryPoint:	00057ECC	Subsystem:	0002
ImageBase:	140000000	NumberOfSections:	0006
SizeOfImage:	001D2000	TimeDateStamp:	517EC665
BaseOfCode:	00001000	SizeOfHeaders:	00000400
BaseOfData:	40000000	Characteristics:	0022
SectionAlignment:	00001000	Checksum:	001868A3
FileAlignment:	00000200	SizeOfOptionalHeader:	00F0
Magic:	020B	NumOfRvaAndSizes:	00000010

Figure 2: Creating new malware using LordPE

LAB SETUP

A lab was setup to simulate the reality of a user receiving an email with a malicious file attached. All platforms in the test were activated with the maximum number of threat prevention services (Anti-Virus, CDR, Threat Emulation) and with the most up-to-date signatures. The Unknown 360 files were a mix of 25% PDF files, 25% EXE files, 25% XLS files, and 25% DOC files. The files were attached to an email that was sent using an unknown, external sender address to a Microsoft 365 email address protected by each of the 3 competing solutions, simulating a real-world email malware attack. Different source email addresses were used to avoid blacklisting of the sender address.

Harmony
Microsoft
mimecast
proofpoint

TEST RESULTS

The combined **known** malware catch rate across all file types is shown in *Figure 3* below. *Figure 4* details **unknown** malicious file test results. As previously mentioned, Check Point Harmony Email & Office was the most successful solution across all file types for **unknown malware**. *Figures 5 & 6* break down the rate of prevention for unknown malicious document and executable file types, respectively. As we see, the expected results are 100% identification of known malware for all solutions.

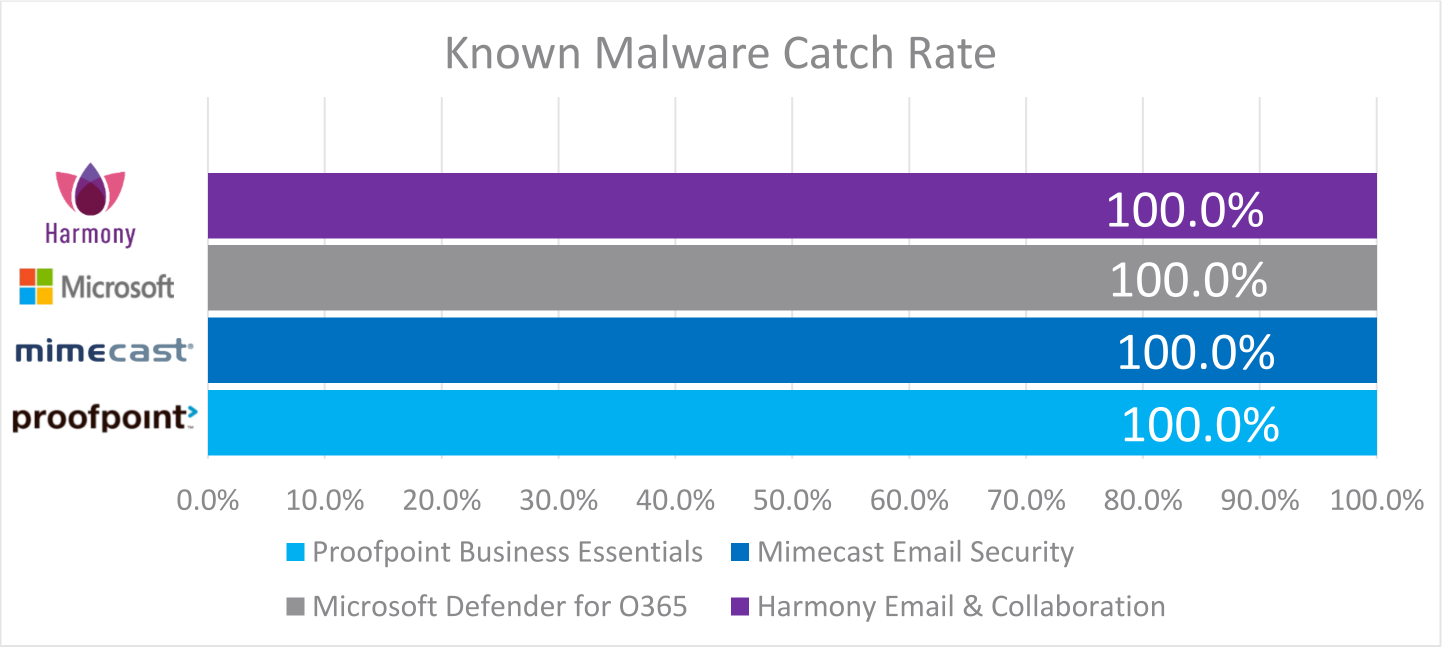


Figure 3: Known malware catch rate

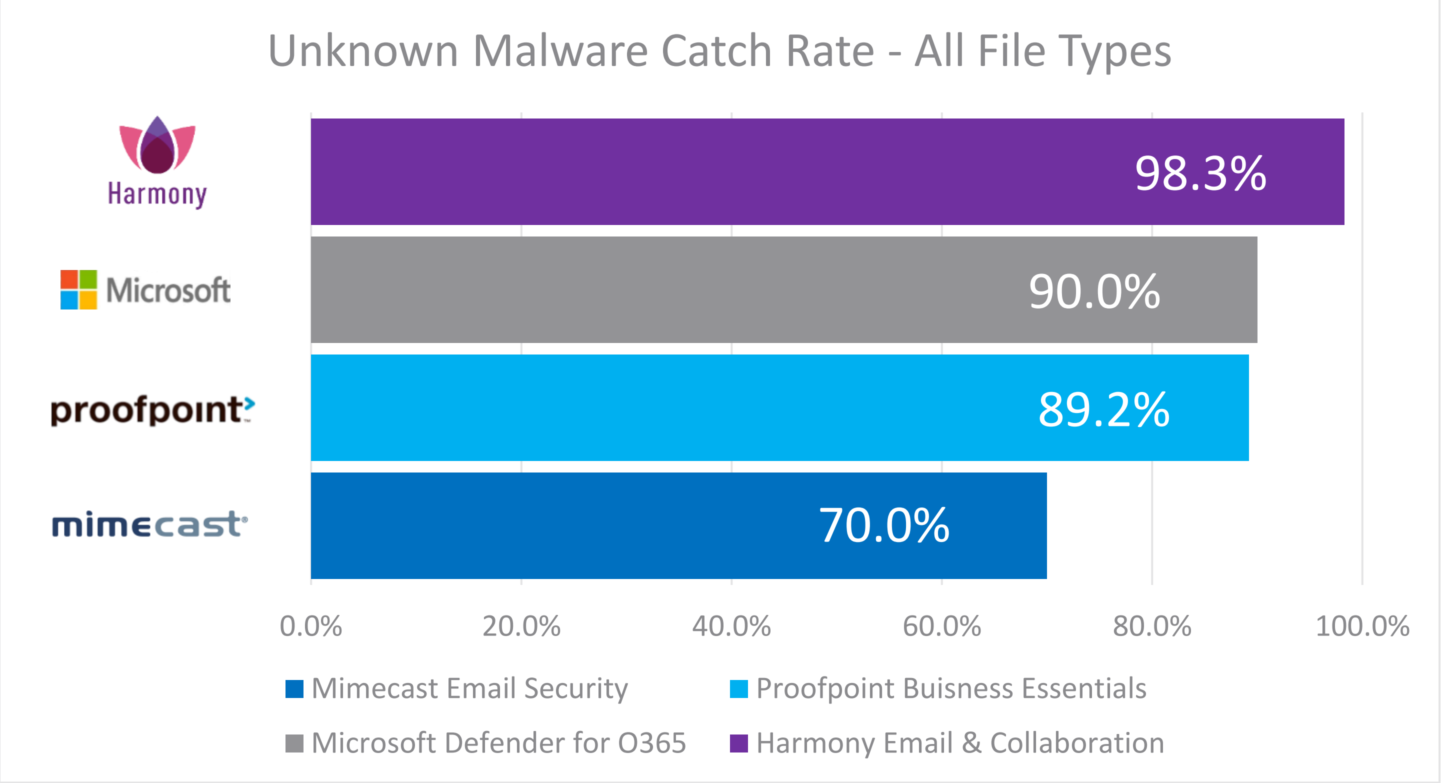


Figure 4: Unknown malware catch rate

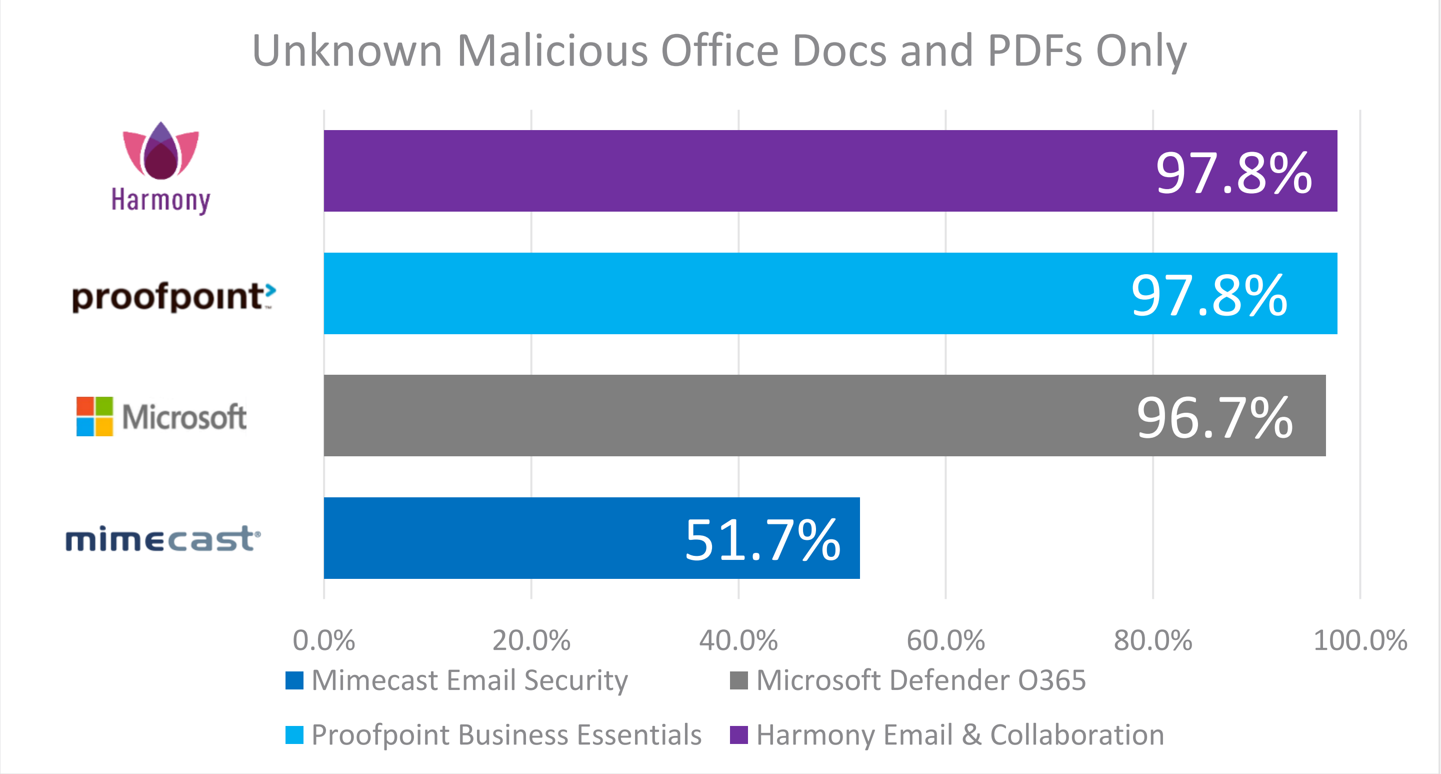
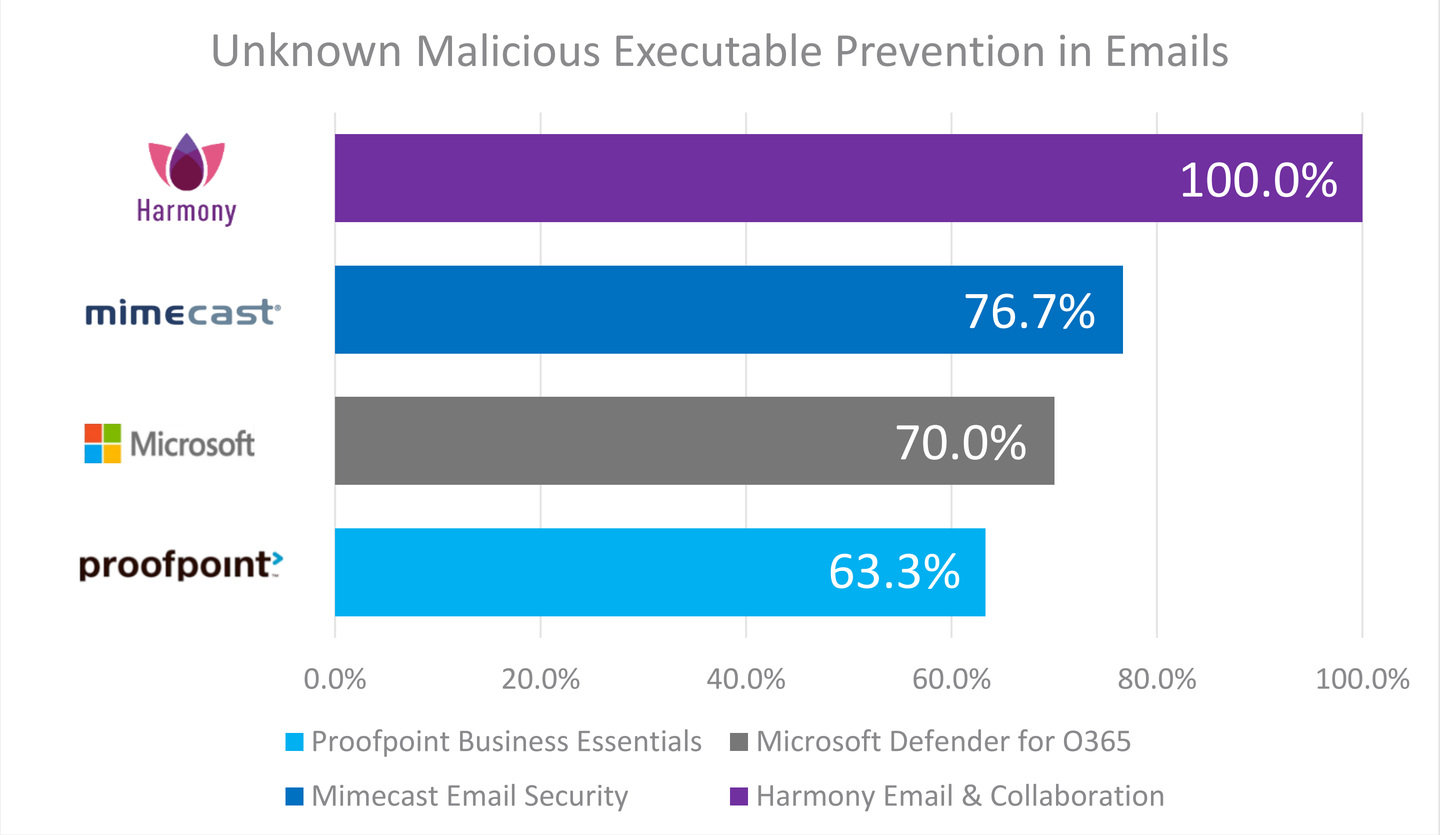


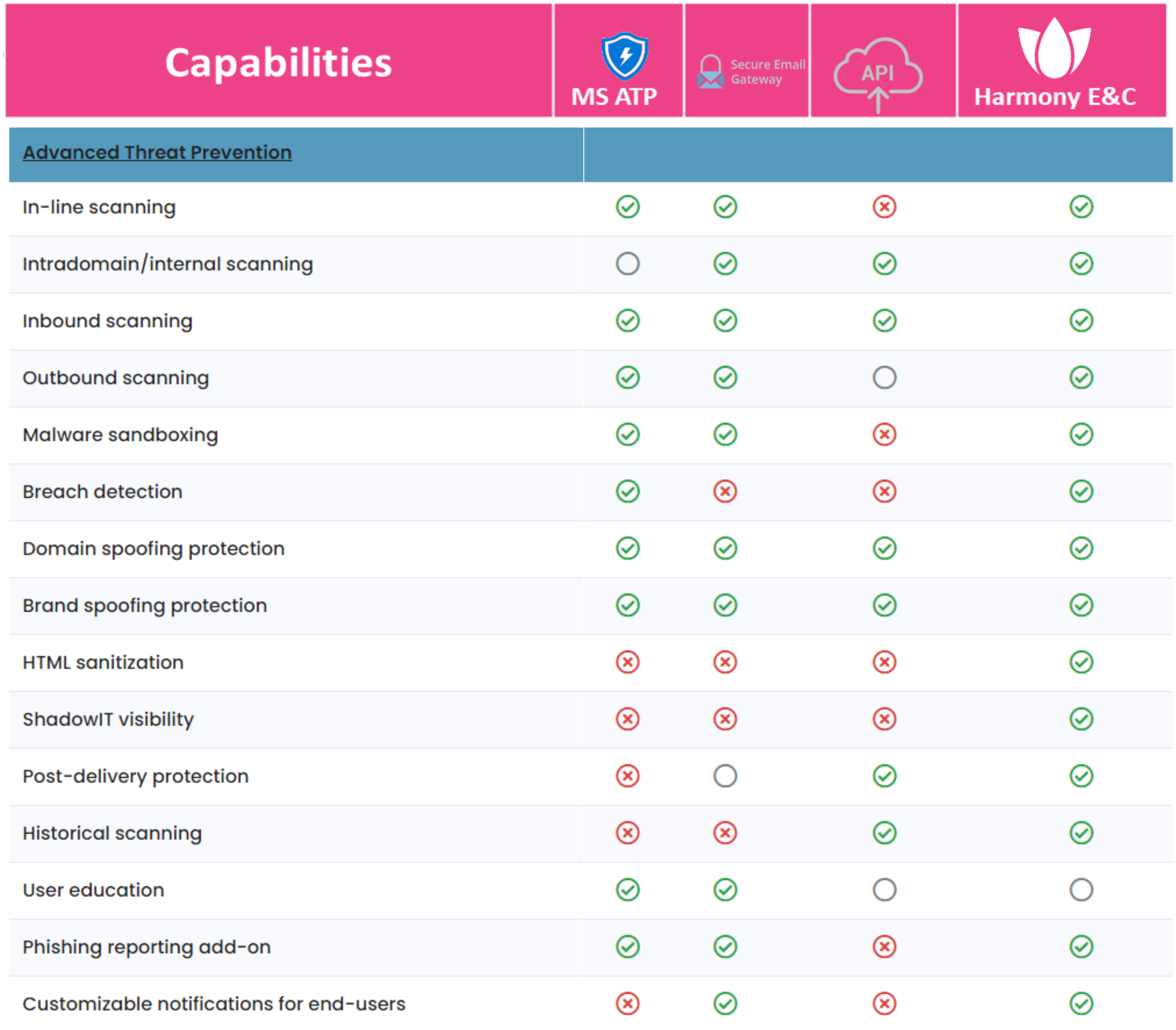
Figure 5: Unknown Malicious documents prevention



DID YOU KNOW? Executables can come in many forms, such as DLL and JavaScript, and they are often embedded in Document files to hide from inspection. (link to source)

Figure 6: Unknown malicious EXE prevention

See below for a brief comparison of the Threat Prevention capabilities of Email Security solutions of all types. For a full capabilities comparison click here.



Capabilities	MS ATP	Secure Email Gateway	API	Harmony E&C
Advanced Threat Prevention				
In-line scanning	✓	✓	✗	✓
Intradomain/internal scanning	○	✓	✓	✓
Inbound scanning	✓	✓	✓	✓
Outbound scanning	✓	✓	○	✓
Malware sandboxing	✓	✓	✗	✓
Breach detection	✓	✗	✗	✓
Domain spoofing protection	✓	✓	✓	✓
Brand spoofing protection	✓	✓	✓	✓
HTML sanitization	✗	✗	✗	✓
ShadowIT visibility	✗	✗	✗	✓
Post-delivery protection	✗	○	✓	✓
Historical scanning	✗	✗	✓	✓
User education	✓	✓	○	○
Phishing reporting add-on	✓	✓	✗	✓
Customizable notifications for end-users	✗	✓	✗	✓

SUMMARY

When it comes to protecting your organization's business email users, it is imperative to choose an email security solution with the industry's best malware catch rate. Your organization's security should not be at risk from the Unknown 360. If you would like to replicate this test, please contact us at EmailSecurity@checkpoint.com.

Detecting and preventing advanced and evasive unknown malware is a challenge that traditional email security solutions aren't up to the task for. And with the rise in ransomware, organizations MUST employ the most advanced protection or run the risk of severe monetary and reputation damage. Phishing protection is also a must for preventing ransomware attacks. See why preventing advanced unknown phishing attacks is key to stopping ransomware here. Check Point and Avanan provide the most advanced email protection on the market, combining a malware catch rate that is far superior to the competition in email security and the most effective anti-phishing in the world!

Get a Demo